

[redacted]

BY ELECTRONIC MAIL

Federal Trade Commission/Office of Secretary
600 Pennsylvania Ave, N.W. – Room H-135 (Annex N)
Washington, DC 20580

RE: Identity Theft Task Force, P065410

Dear Task Force:

I would like to offer several brief comments on the first two bullet points of your areas of focus--keeping sensitive data out of the hands of identity thieves and making it more difficult for thieves to use information to steal identities. I am an attorney who specializes in privacy and identity theft matters and I lecture to bar and trade association groups on these subjects. While I am formally employed in the private sector, these comments are my own alone and are not submitted on behalf of my employer or any other entity.

I was also an early victim of identity theft in 1993. While it took me in excess of 500 hours and close to seven years to re-establish my credit, I will not comment on victim recoveries or law enforcement. The identity theft problem in this country is systematically driven and I believe the problem of identity theft can be largely mitigated through several relatively simple systematic changes in our laws or regulations, politically difficult as some may be.

I support increased activity by law enforcement in pursuing identity thieves but dealing with this problem one-by-one is not going to be cost effective or make a material change in the explosion of this crime absent increased staffing and expense in the law enforcement sector. That is why systematic solutions are necessary and far more effective than raising criminal penalties or hiring additional prosecutors

Social Security Numbers

The lynchpin of identity theft is the use by identity thieves of Social Security numbers. If Social Security numbers were less susceptible to theft and, if stolen, less susceptible to being used by persons other than the actual person to whom a Social Security number is assigned, identity theft would be substantially mitigated.

Unfortunately, government and business practices today make the opposite true. Government entities and private companies (especially insurance companies) use Social Security numbers as identifiers. Whenever a person communicates their Social Security number, the risk of that number being compromised rises substantially. A record of it is made, persons are able to access it, hackers can gain

unauthorized access, and the information transmitted to others multiple times, all without the person knowing or having any reason to suspect untoward activity. No system can effectively preclude access once a Social Security number is communicated. The key is to limit use of Social Security numbers and take steps to preclude their use by persons other than the person to whom the number is rightfully assigned.

The first step is simple. Prohibit the communication or use of Social Security numbers as identifiers or with respect to any but a limited number of communications, principally law enforcement or Social Security benefits related. New York recently passed a law in this regard that I think attempts to reach this goal. I attach a copy of that law. While I understand industries such as the credit industry and health insurers have used Social Security numbers to establish databases, the risk to consumers outweighs the IT commitment necessary to restructure those databases.

Any entity that uses a Social Security number should be required to encrypt it and use two factor authentication to identify any attempted use of the Social Security number. "Out of wallet" questions based on prior experiences of the legitimate owner with the would-be user that were previously verified provide a basis for this and replicate what credit bureaus sell today as enhanced personal identification services. Insurers could do the same thing with prior claims histories. Less favorable would be "shared secrets" as these can be tracked by keylogging viruses. Any government or industry that uses Social Security numbers as identifiers has a wealth of data from which to generate these out of wallet questions and must undertake to do so. (E.g., the Social Security Administration could ask a proposed user where they lived when their number was issued, the names of their grandparents, and how many siblings they have).

The second step is to stop a vicious cycle that encourages the use of compromised Social Security numbers by illegal immigrants and others seeking to establish identities. Each year, the Social Security Administration reports 9 million persons to the IRS and remits tax withholdings, on people with the wrong Social Security number. (These withholdings have totaled over \$550 billion since 1986 and go into an Earnings Suspense Fund at the Social Security Administration that is used as part of its funding.) The Social Security Administration has determined that food service and farming industries generate the bulk of these "no-match" situations. Credit bureaus establish multiple consumer files on one Social Security number but will not inform consumers if another person is using their Social Security number. Employers are not prosecuted for failing to verify the legitimacy of employee Social Security numbers and do not do so for the purpose of obtaining access to cheap illegal immigrant labor.

As a result, people assume identities using a stolen Social Security number and no one in authority or power has any interest in doing anything about it. The legitimate owner of the Social Security number learns only years later when they are denied a job, pursued by collectors, or contacted by law enforcement for the wrongful activities of the identity thief. Prior to that time, the rightful person may suffer indirectly as the wrongful user's credit experiences may be unintentionally factored into the rightful person's credit score. This happened to me fairly recently. I was told my credit score was lower than it should have been because of numerous new accounts being opened, none of which appeared on my credit reports (I have only opened two credit accounts since 2002). However, my efforts to resolve this discrepancy were met with a dead end at the credit bureaus. I and my family continue to suffer an

unnecessarily high cost of credit and insurance. So do millions of other Americans. Refining credit scoring models would only address a symptom, not the entire problem.

Addressing the use of legitimate Social Security numbers by identity thieves seeking to live under that number will meet resistance by immigrant rights groups (who seem to feel stealing a Social Security number is legitimate for an illegal immigrant to get work in the U.S.), the Social Security Administration (who estimated the Earnings Suspense Account loss would lead to a 10% shortfall in its funding needs), credit bureaus (who continue to profit exorbitantly at consumers' expense by establishing purportedly legitimate credit files for the identity thieves--for a high price, credit bureaus will sell certain credit report users a service that indicates whether multiple credit files exist for a Social Security number but only on express condition that it not be disclosed to the consumer), and employers (who want access to cheap illegal labor). However, it is the U.S. consumer who suffers by this de facto legitimization of identity theft by our government and the private sector. This is a tremendous injustice that I urge the Task Force to identify and correct notwithstanding the resistance you will encounter.

In this regard, I believe credit bureaus are a large cause—if not the primary cause--of the identity theft in this country because of their enthusiastic embrace of identity theft activity (by establishing credit files for multiple persons with the same Social Security numbers, the credit bureaus know they are facilitating identity theft) and their unwillingness to build any logic (such as identifying patterns of suspicious credit file activity) to alert the consumer to mitigate the problem. The credit bureaus' flat out refusal to inform consumers if other persons are using their Social Security number (at any price) is socially unconscionable. The credit bureaus' propagating and trafficking in illegal data that enables identity theft is a primary enabler of the problem. The Task Force needs to address the institutionalized recklessness of credit bureaus, acknowledge their responsibility for these activities that perpetuate identity theft, and act to stop it. By preventing credit bureaus from opening files for more than one person per Social Security number and by requiring credit bureaus to verify that the file for that Social Security number is the correct person—today, credit bureaus willingly open credit files for persons using children's Social Security numbers to the point that children represent up to 5% of identity theft victims—and requiring credit bureaus to contact the correct person when suspicious activity occurs, identity theft could be mitigated in a way that adding 10,000 prosecutors could not. Credit bureaus are literally partners in the commission of identity theft and they have shown repeatedly that they will not act in consumers' best interest except under the threat or requirement of law.

Another important element is to grant nationally the right of consumers to freeze their credit files. A security freeze represents a consumer's best protection against an identity thief particularly if the consumer is vigilant about monitoring their existing accounts. A credit file freeze will cut an identity thief off at the outset. However, my recommendation for a national right to freeze one's credit file goes a step further. Consumers must also be informed when they freeze a file whether or not another person is using their Social Security number. Upon showing adequate proof of identity and the validity of their Social Security number (this could be done through documentation or by means of a verification process with the Social Security Administration), the credit bureau would be mandated to report to the consumers the other persons who are using their Social Security number and the credit bureau should then be forced to report to credit users that those files have been verified to be illegitimate. Law enforcement should have the ability and means to investigate and prosecute the additional users.

I realize the credit bureau lobby is substantial and will vigorously oppose these reforms. Their vigorous opposition to security freeze rights demonstrates their disinterest in helping consumers avoid becoming identity theft victims. However, I hope the Task Force has the wisdom to understand and the courage to act. Information breeds identity theft and the system makes identity theft an easy, profitable crime. The problem must be addressed systematically. Only these systematic reforms can effectuate meaningful change.

Medical Identity Theft

A final word if I may about medical identity theft. Consumer information is way too broadly distributed and made available in the world of healthcare providers, insurers, consultants, and others. Again, with every communication of personal information, the potential for identity theft increases substantially. At minimum, consumers should be permitted to see and correct their HIPPA files and the same prohibitions on establishing multiple files using the same Social Security number should be implemented in this arena. Identity theft can lead to devastating financial impact, both directly and indirectly, but medical identity theft can lead to death. I urge the Task Force to consider medical identity theft reform measures as an independent area of review and policy given its more dire consequences.

Thank you for considering my comments. Should you wish additional information or want to contact me, please call me during business hours at [redacted]. I applaud your efforts and am gratified that our government is taking this initiative to address the 21st Century's most prevalent crime.

Sincerely,

[redacted]